

U.S. Application No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

2

### REMARKS

Claims 1 and 5-36 are all the claims presently pending in the application. No claims are amended and no new matter is added.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza (U.S. Patent No. 6,446,210) in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon").

These rejections are respectfully traversed in the following discussion.

#### **I. REQUEST FOR NEW OFFICE ACTION**

It is noted that the Examiner's Response to Arguments is identical to the previous Response to Arguments, except for stating that "[t]he Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands" (see Office Action at page 2, paragraph 5). In fact, with respect to the text of each of the rejections in the present Office Action (i.e., the rejection under 35 U.S.C. § 101 and 35 U.S.C. § 103), the above statement at paragraph 5 of the present Office Action is the only change from the previous Office Action.

Applicant notes that, where Applicant traverses any rejections, the Examiner should, if he repeats the rejection, take note of the Applicant's argument and answer the substance of it (see M.P.E.P. § 707.07(f)).

U.S. Application No. 09/457,732 3  
Docket No. YOR919990137US1  
(YOR.080)

In the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, Applicant clearly rebutted each of the Examiner's positions. However, the Examiner did not respond to Applicant's traversal arguments, with the exception of the statement mentioned above. Applicant reiterates those traversal positions below.

Applicant respectfully submits that the Examiner should have responded to all of Applicant's traversal positions and answered the substance of the arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)).

Applicant submits that the present Office Action fails to advance the prosecution of the present application.

A Petition for a New Office Action, which properly responds to each of Applicant's traversal positions and answers the substance of those arguments, concurrently is submitted herewith.

## II. THE CLAIMED INVENTION

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P').

U.S. Application No. 09/457,732 4  
Docket No. YOR919990137US1  
(YOR.080)

Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

### III. REJECTION UNDER 35 U.S.C. § 101

Claims 1, 14-16, 31, and 32 also stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility. That is, the Examiner asserts that the claimed invention "could not work", as evidenced by the Handbook of Applied Cryptography.

Applicants respectfully disagree with each of the Examiner's positions, for the following reasons.

A. First, it is noted that the Examiner's Response to Arguments is identical to the previous Response to Arguments, except for stating that "[t]he Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands" (see Office Action at page 2, paragraph 5), as mentioned above.

However, such clearly is not sufficient for responding to each of Applicant's traversal positions, as required by M.P.E.P. § 707.07(f) and § 2144.08(III).

Hence, Applicants respectfully submit that the Examiner should have responded to all of Applicant's traversal positions and answered the substance of the arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)).

U.S. Application No. 09/457,732 5  
Docket No. YOR919990137US1  
(YOR.080)

B. Second, Applicants reiterate that the Examiner is misunderstanding the invention and Applicants' traversal arguments, and has misapplied the teachings of the Handbook of Applied Cryptography.

Applicant reiterates that the disclosure of the present application explicitly acknowledges the problem that a simple hash function approach would not work (as disclosed in the above Handbook and suggested by the Examiner in the present Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).

That is, the specification of the present application (at page 16, lines 15-17) specifically states that:

Because  $P0$  is in general (possibly) slightly different from  $Pi$  for  $i > 0$ , the secret version of  $p0$  will generally be quite different from the secret version of  $Pi$ . This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data under uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods to circumvent this situation and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first, second, and third methods for circumventing the very problem with comparing encrypted or hash data which the Examiner mentions.

U.S. Application No. 09/457,732 6  
Docket No. YOR919990137US1  
(YOR.080)

Thus, the Examiner's continued assertion that the invention is inoperable because of the teachings of the Handbook of Applied Cryptography and section 9.2.2 Basis Properties and Definitions clearly is erroneous, as a matter of both fact and law. That is, the Examiner has failed to consider the specific disclosure of the present application, which clearly describes a novel solution for circumventing the problem being relied upon by the Examiner in the Handbook of Applied Cryptography.

Indeed, the disclosure of the present application clearly does not contradict the teachings of the Handbook of Applied Cryptography, upon which the Examiner relies.

Instead, the present invention clearly explains a method of circumventing the very problems which the Handbook of Applied Cryptography identifies and for which the Handbook is being relied upon by the Examiner as teaching.

Indeed, the Examiner has erroneously interpreted what the invention teaches in a way that clearly does not comport with the actual disclosure of the present application.

For example, in paragraph 11 of the present Office Action, the Examiner states that the claims "*generally relate to ...*". However, the Examiner's position clearly fails to consider all of the teachings of the invention (i.e., the actual disclosure of the present application), or for that matter, the specific features recited in the claims.

As Applicants have explained in each of the previous Amendments, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines

U.S. Application No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

7

whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Indeed, the claimed invention does not merely "generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication", as alleged by the Examiner.

That is, the claimed invention does NOT use a hash function by ITSELF to authenticate two samples, as erroneously alleged by the Examiner. Instead, a hash function is only part of the novel solution provided by the present invention for circumventing the identified problems with the prior art.

Moreover, not all of the claims deal with imperfect biometric data. Instead, only some of the claims deal with such imperfect data.

For the foregoing reasons, Applicants respectfully submit that the claimed invention could (and does) work for its intended purpose, as disclosed in the disclosure of the present application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20, line 8).

Moreover, the present application specifically states that the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering

U.S. Application No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

8

the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Applicants respectfully submit that claims 1, 14-16, 31, and 32: (1) are supported by a specific and substantial asserted utility or a well established utility, (2) are not inoperative and do not lack utility, and (3) could (and do) work for their intended purpose, as disclosed in the disclosure of the specification of the present application, for example, at page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

To summarize, the Examiner clearly has not responded to all of Applicant's traversal positions and answered the substance of the above traversal arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)). Moreover, the Examiner appears to have erroneously summarized the teachings of the present invention in a way which clearly does not comport with the actual disclosure of the invention. Indeed, the present invention clearly is not contrary to the teachings of the Handbook of Applied Cryptography, but instead,

U.S. Application No. 09/457,732 9  
Docket No. YOR919990137US1  
(YOR.080)

acknowledges the very problem identified in the Handbook by the Examiner and provides a novel solution for circumventing such problems.

Thus, the Examiner's assertion that "Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands" (see Office Action at page 2, paragraph 5) clearly is inappropriate, and indeed, is not germane to the rejections since the Examiner has not explained or provided any reasons as to why the actual disclosure of the present application would be inoperative and lack utility.

For the foregoing reasons, Applicants respectfully submit that a person of ordinary skill in the art to which the invention pertains would recognize the utility of the claimed invention and would know and understand the claimed invention. Thus, the Examiner is requested to reconsider and withdraw this rejection.

#### **IV. THE PRIOR ART REJECTION**

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon. Applicants respectfully traverse this rejection, for at least the following reasons.

For the Examiner's convenience, the traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, and the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005 are incorporated herein by reference in their entirety.



U.S. Application No. 09/457,732 10  
Docket No. YOR919990137US1  
(YOR.080)

In the "Response to Arguments" section of the Office Action, the Examiner continues to allege that the features upon which Applicants rely are not recited in the claims (see Office Action at page 3, paragraph 6). However, Applicants submit that the traversal arguments which are set forth at least in the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005 and the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, clearly point out the claimed subject matter which is clearly and particularly defined, for example, by independent claim 1.

Also, in the "Response to Arguments" section of the Office Action, the Examiner relies on M.P.E.P. § 2122 as stating that, when a reference relied upon expressly anticipates or makes obvious all of the elements of the claimed invention, the reference is presumed to be operable.

However, as Applicants have pointed out, Borza does not expressly anticipate or make obvious all of the elements of the claimed invention. Thus, irrespective of the operability of Borza, Applicants submit that the alleged combination of Borza and Kharo do not disclose or suggest all of the features of the claimed invention.

That is, Borza only generally mentions that a comparison of encrypted data is done, but does not disclose the specific features recited in the claimed invention. In fact, Borza clearly does not discuss how it compares encrypted data.

In fact, the cited portion of Borza at column 16, lines 31-38 does not determine whether  $h(P)$  is close to  $h(P')$ , as alleged by the Examiner. Indeed, it is unclear how Borza at column 16, lines 31-38 even relates to the disclosure of comparing encrypted data against an encrypted template at column 8, lines 28-38.

U.S. Application No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

11

That is, nowhere at column 16, lines 31-38, or in Figure 13 which is being described, does Borza mention comparing encrypted data against an encrypted template. Thus, the Examiner has mischaracterized the teachings of Borza.

Even assuming *arguendo* that Borza is operative, the disclosure provided by Borza fails to teach or suggest all of the features of the claimed invention for which it is being relied upon. Therefore, the alleged combination of Borza and Kharo clearly does not disclose or suggest all of the features of the claimed invention.

In other words, irrespective of the operability of Borza, the disclosure of Borza clearly does not disclose or suggest *how* to compare two encrypted data sets to determine similarity between the two original data sets according to the features recited in the claimed invention.

Applicants reiterate that the ordinarily skilled artisan would understand that encryption causes diffusion of data, which means that the encryption of two similar, but not identical data sets create two encrypted data sets that are very different. Thus, merely comparing two encrypted data sets still would not (and does not) disclose or suggest the similarity between the two unencrypted data sets.

In fact, as the Examiner points out, and as Applicants specifically acknowledge in the specification, no identification is possible by direct comparison of the encrypted data.

Thus, in contrast to Borza, the claimed invention discloses several approaches to compare encrypted or hashed data under uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8).

U.S. Application No. 09/457,732 12  
Docket No. YOR919990137US1  
(YOR.080)

Specifically, as mentioned above, the disclosure of the present invention specifically acknowledges the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).

For example, the specification of the present application (at page 16, lines 15-17) specifically states that:

Because  $P0$  is in general (possibly) slightly different from  $Pi$  for  $i > 0$ , the secret version of  $p0$  will generally be quite different from the secret version of  $Pi$ . This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data under uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods to circumvent this situation and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first, second, and third methods for circumventing the very problem with comparing encrypted or hash data which the Examiner mentions.

The claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed

U.S. Application No. 09/457,732 13  
Docket No. YOR9199901371US1  
(YOR.080)

invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

The present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the claimed invention solves the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11) (e.g., see specification at page 16, lines 15-17) by circumventing the problem, as disclosed and claimed.

For the foregoing reasons, Borza clearly does not disclose or suggest at least "to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P", as recited in claim 1.

On the other hand, Applicants respectfully reiterate that Kharon does not make up for the deficiencies of Borza.

The Examiner relies on Kharon for teaching the claimed "extracting sub-collections S<sub>j</sub> from the collection of data in data set P; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections S<sub>j</sub> with those data stored in said database, wherein if one or more of the sub-collection S<sub>j</sub> matches with said data, then verification is deemed to have occurred", as recited in independent claim 1.

U.S. Application No. 09/457,732 14  
Docket No. YOR919990137US1  
(YOR.080)

However, contrary to the Examiner's position, Kharon (at column 13, lines 43-67) does not describe extracting multiple subsets  $S_j$  (i.e., "sub-collections") from the data. Furthermore, Kharon does not describe encrypting a number of such subsets (i.e., a "number of such sub-collections") such that at least one is reproduced exactly with a predetermined probability.

Applicants respectfully submit that the Examiner seems to have confused using a smaller section of the data for verification (which would be less desirable since less data is used), whereas the claimed invention uses multiple subsets of the data for verification.

Thus, using just a smaller subset of the data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data.

On the other hand, using multiple subsets of the data, according to the claimed invention, allows encrypted data to be compared and to generate a measure of similarity.

Thus, for the foregoing reasons, Applicants respectfully reiterate that neither Borza nor Kharon discloses or suggests all of the features of the claimed invention. Therefore, the Examiner is requested to reconsider and withdraw this rejection.

## V. CONCLUSION

In view of the foregoing, Applicants submit that claims 1 and 5-36, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.


U.S. Application No. 09/457,732 15  
Docket No. YOR919990137US1  
(YOR.080)

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: May 8, 2006


  
John J. Dresch, Esq.  
Registration No. 46,672

Sean M. McGinn, Esq.  
Registration No. 34,386

**MCGINN INTELLECTUAL PROPERTY  
LAW GROUP, PLLC**  
8321 Old Courthouse Road, Suite 200  
Vienna, Virginia 22182-3817  
(703) 761-4100  
Customer No. 21254

**CERTIFICATE OF TRANSMISSION**

I certify that I transmitted via facsimile to (571) 273-8300 the enclosed Request for Reconsideration under 37 C.F.R. § 1.116 to Examiner Christian A. La Forgia on May 8, 2006.

  
John J. Dresch, Esq.  
Registration No. 46,672